PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – GRSIC

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Art. 6º da Lei nº 10.683, de 28 de maio de 2003.
Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
Norma Complementar 01/DSIC/GSIPR de 13 de outubro de 2008.
Norma Complementar 02/DSIC/GSIPR de 13 de outubro de 2008.
ABNT NBR ISO/IEC 27001:2006.
ABNT NBR ISO/IEC 27005:2008.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

2 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

3.1 **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

3.2 **Análise de riscos** – uso sistemático de informações para identificar fontes e estimar o risco;

3.3 **Análise/avaliação de riscos** – processo completo de análise e avaliação de riscos;

3.4 **Ativos de Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

3.5 **Avaliação de riscos** – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

3.6 **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

3.7 **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e consequências de um risco;

3.8 **Evitar risco** – uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

3.9 **Gestão de Riscos de Segurança da Informação e Comunicações** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

3.10 **Identificação de riscos** – processo para localizar, listar e caracterizar elementos do risco;

3.11 **Reduzir risco** – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

3.12 **Reter risco** – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

3.13 **Riscos de Segurança da Informação e Comunicações** – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

3.14 **Transferir risco** – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

3.15 **Tratamento dos riscos** – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

3.16 **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão ou entidade da Administração Pública Federal, direta e indireta – APF, além de estarem alinhadas à respectiva Política de Segurança da Informação e Comunicações do órgão ou entidade;

4.2 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações;

4.3 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, publicada no Diário Oficial da União nº 199, Seção 1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua;

4.4 A Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios.

5 PROCEDIMENTOS

Nos itens abaixo será apresentada uma abordagem sistemática do processo Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, com o objetivo de manter os riscos em níveis aceitáveis. Esse processo é composto pelas etapas de definições preliminares, análise/avaliação dos riscos, plano de tratamento dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração e análise crítica, melhoria do processo de Gestão de Riscos de Segurança da Informação e Comunicações e comunicação do risco, conforme apresentado no **Anexo A** desta Norma.

5.1 **Definições preliminares:** nesta fase, deve-se realizar uma análise da organização visando estruturar o processo de gestão de riscos de segurança da informação e comunicações, sendo consideradas as características do órgão ou entidade e as restrições a que estão sujeitas. Esta análise inicial permite que os critérios e o enfoque da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC sejam os mais apropriados para o órgão, apoiando-o na definição do escopo e na adoção de uma metodologia.

5.1.1 Definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC a fim de delimitar o âmbito de atuação. Esse escopo pode abranger o órgão ou entidade como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação;

5.1.2 Adotar uma metodologia de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.

5.2 **Análise/avaliação dos riscos:** nesta fase, inicialmente serão identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados.

5.2.1 Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido;

5.2.2 Identificar os riscos associados ao escopo definido, considerando:

a) as ameaças envolvidas;
b) as vulnerabilidades existentes nos ativos de informação;
c) as ações de Segurança da Informação e Comunicações – SIC já adotadas.

5.2.3 Estimar os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados;

5.2.4 Avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos no item 5.1.2;

5.2.5 Relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo órgão ou entidade.

5.3 **Plano de Tratamento dos Riscos**

5.3.1 Determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco, observando:

a) a eficácia das ações de Segurança da Informação e Comunicações – SIC já existentes;
b) as restrições organizacionais, técnicas e estruturais;
c) os requisitos legais;
d) a análise custo/ benefício.

5.3.2 Formular um plano para o tratamento dos riscos, relacionando, no mínimo, as ações de Segurança da Informação e Comunicações – SIC, responsáveis, prioridades e prazos de execução necessários à sua implantação.

5.4 **Aceitação do Risco:** verificar os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

5.5 **Implementação do Plano de Tratamento dos Riscos:** executar as ações de Segurança da Informação e Comunicações – SIC incluídas no Plano de Tratamento dos Riscos aprovado.

5.6 **Monitoração e análise crítica:** detectar possíveis falhas nos resultados, monitorar os riscos, as ações de Segurança da Informação e Comunicações – SIC e verificar a eficácia do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC.

5.6.1 Do processo de gestão: monitorar e analisar criticamente o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC de forma a mantê-lo alinhado às diretrizes gerais estabelecidas e às necessidades do órgão ou entidade;

5.6.2 Do risco: manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos;
b) no ambiente;
c) nos ativos de informação;
d) nas ações de Segurança da Informação e Comunicações – SIC;
e) nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).

5.7 **Melhoria do Processo de GRSIC**

5.7.1 Propor à autoridade decisória do órgão ou entidade a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica;

5.7.2 Executar as ações corretivas ou preventivas aprovadas;

5.7.3 Assegurar que as melhorias atinjam os objetivos pretendidos.

5.8 **Comunicação do Risco:** manter as instâncias superiores informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas.

6 RESPONSABILIDADES

6.1 Cabe à Alta Administração do órgão ou entidade da Administração Pública Federal, direta e indireta – APF aprovar as diretrizes gerais e o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC observada, dentre outras, a respectiva Política de Segurança da Informação e Comunicações;

6.2 Os Gestores de Segurança da Informação e Comunicações, no âmbito de suas atribuições, são responsáveis pela coordenação da Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

6.3 De acordo com as necessidades de cada órgão ou entidade, os Gestores de Segurança da Informação e Comunicações poderão indicar responsáveis pelo gerenciamento de atividades, a quem serão conferidas, no mínimo, as seguintes atribuições:

6.3.1 análise/avaliação e tratamento dos riscos;

6.3.2 elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações, em cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração.

7 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.

8 ANEXO

A - Processo de Gestão de Riscos de Segurança da Informação e Comunicações

ANEXO A

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES